CLAIMS

1. A method for processing communication traffic, comprising:

monitoring the communication traffic that is directed to a group of addresses on a network;

determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group;

detecting a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, such that the deviation is indicative that at least some of the communication traffic may be of malicious origin; and

responsively to detecting the deviation, filtering the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin.

2. The method according to claim 1, wherein monitoring the communication traffic comprises selecting a subset of the group of the addresses to monitor responsively to the baseline characteristics.

3. The method according to claim 2, wherein determining the respective baseline characteristics comprises determining respective amounts of the communication traffic that are directed to the addresses in the group, and wherein selecting the subset comprises selecting the addresses in the subset such that the addresses in the subset receive relatively small amounts of the communication traffic by comparison with other addresses in the group.

4. The method according to claim 1, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic.

5. The method according to claim 1, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed.

6. The method according to claim 1, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic.

7. The method according to claim 1, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group.

8. The method according to claim 1, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic.

9. The method according to claim 8, wherein detecting the deviation comprises reading a Time-To-Live (TTL) field in headers of data packets sent to the addresses in the group, and detecting a change in values of the TTL field relative to the baseline characteristics.

10. The method according to claim 1, wherein detecting the deviation comprises detecting events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network.

11. The method according to claim 10, wherein detecting the events comprises detecting failures to establish a Transmission Control Protocol (TCP) connection.

12. The method according to claim 1, and comprising receiving packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to receiving the packets.

13. The method according to claim 12, wherein receiving the packets comprises receiving Internet Control Message Protocol (ICMP) unreachable packets.

14. The method according to claim 1, wherein monitoring the communication traffic comprises making a determination that one or more packets transmitted over the network are ill-formed, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to the ill-formed packets.

15. The method according to claim 1, wherein detecting the deviation comprises incrementing a count of events that are indicative of the malicious origin of the communication traffic, and deciding whether to filter the communication traffic responsively to the count.

16. The method according to claim 15, wherein detecting the deviation comprises receiving data packets of potentially malicious origin, each data packet having a respective source address and destination address, and wherein incrementing the count comprises determining an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least one data packet

had the same respective source address and at least one data packet had the same respective destination address.

17. The method according to claim 16, wherein determining the amount by which to increment the count comprises incrementing the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address.

18. The method according to claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein filtering the communication traffic comprises intercepting the communication traffic of the detected type.

19. The method according to claim 18, wherein detecting the type comprises determining at least one of a communication protocol and a port that is characteristic of the communication traffic.

20. The method according to claim 18, wherein detecting the type comprises determining one or more source addresses of the communication traffic that appears to be of the malicious origin, and intercepting the communication traffic sent from the one or more source addresses.

21. The method according to claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein monitoring the communication traffic

comprises collecting specific information relating to the traffic of the detected type.

22. The method according to claim 21, wherein collecting the specific information comprises determining one or more source addresses of the traffic of the detected type.

23. The method according to claim 1, wherein monitoring and filtering the communication traffic comprise monitoring and filtering the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

24. The method according to claim 23, and comprising monitoring the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program.

25. A method for processing communication traffic, comprising:

monitoring the communication traffic originating from a group of addresses and passing through a selected node on a network;

detecting a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses; and

tracing a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running.

26. The method according to claim 25, wherein tracing the route comprises identifying a port of a switch on the network to which the computer is connected, and comprising disabling the identified port.

27. The method according to claim 25, wherein detecting the pattern comprises determining that the computer has transmitted packets to a large number of different destination addresses.

28. The method according to claim 25, wherein detecting the pattern comprises detecting a large number of packets transmitted by the computer to a specified port.

29. A method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection;

detecting an increase in a rate of arrival of the packets that are indicative of the communication failure; and

responsively to the increase, filtering the communication traffic so as to remove at least some of the communication traffic that is generated by the worm infection.

30. The method according to claim 29, wherein monitoring the communication traffic comprises detecting Internet Control Message Protocol (ICMP) unreachable packets.

31. The method according to claim 29, wherein monitoring the communication traffic comprises detecting failures to

establish a Transmission Control Protocol (TCP) connection.

32. A method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect ill-formed packets;

making a determination, responsively to the ill-formed packets, that at least some of the communication traffic has been generated by a worm infection; and

responsively to the determination, filtering the communication traffic so as to remove the at least some of the communication traffic that is generated by the worm infection.

33. The method according to claim 32, wherein the packets comprise a header specifying a communication protocol, and wherein monitoring the communication traffic comprises determining that the packets contain data that are incompatible with the specified communication protocol.

34. The method according to claim 32, wherein the packets comprise a header specifying a packet length, and wherein monitoring the communication traffic comprises determining that the packets contain an amount of data that is incompatible with the specified packet length.

35. Apparatus for processing communication traffic, comprising a guard device, which is adapted to monitor the communication traffic that is directed to a group of addresses on a network, to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group, to detect a deviation from the respective baseline characteristics

of the communication traffic directed to at least one of the addresses in the group, such that the deviation is indicative that at least some of the communication traffic may be of malicious origin, and responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin.

36. The apparatus according to claim 35, wherein the guard device is adapted to select a subset of the group of the addresses to monitor responsively to the baseline characteristics.

37. The apparatus according to claim 36, wherein the respective baseline characteristics are indicative of respective amounts of the communication traffic that are directed to the addresses in the group, and wherein the guard device is adapted to select the addresses in the subset such that the addresses in the subset receive relatively small amounts of the communication traffic by comparison with other addresses in the group.

38. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic.

39. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed.

40. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic.

41. The apparatus according to claim 35, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group.

42. The apparatus according to claim 35, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic.

43. The apparatus according to claim 42, wherein the guard device is adapted to read a Time-To-Live (TTL) field in headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems.

44. The apparatus according to claim 35, wherein the guard device is adapted to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network.

45. The apparatus according to claim 44, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection.

46. The apparatus according to claim 35, wherein the guard device is adapted to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets.

47. The apparatus according to claim 46, wherein the packets comprises Internet Control Message Protocol (ICMP) unreachable packets.

48. The apparatus according to claim 35, wherein the guard device is adapted to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets.

49. The apparatus according to claim 35, wherein the guard device is adapted to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count.

50. The apparatus according to claim 49, wherein the guard device is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, and is adapted to determine an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address.

51. The apparatus according to claim 40, wherein the guard device is adapted to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address.

52. The apparatus according to claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by

intercepting the communication traffic of the detected type.

53. The apparatus according to claim 52, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port.

54. The apparatus according to claim 52, wherein the guard device is adapted to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses.

55. The apparatus according to claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type.

56. The apparatus according to claim 55, wherein the specific information comprises one or more source addresses of the traffic of the detected type.

57. The apparatus according to claim 35, wherein the guard device is adapted to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

58. The apparatus according to claim 57, wherein the guard device is adapted to monitor the communication traffic that is transmitted by computers in the protected

area so as to detect an infection of one or more of the computers by a malicious program.

59. Apparatus for processing communication traffic, comprising a guard device, which is adapted to monitor the communication traffic originating from a group of addresses and passing through a selected node on a network, to detect a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses, and to trace a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running.

60. The apparatus according to claim 59, wherein the guard device is adapted to identify a port of a switch on the network to which the computer is connected, and to instruct the switch to disable the identified port.

61. The apparatus according to claim 59, wherein the guard device is adapted to detect the pattern by determining that the computer has transmitted packets to a large number of different destination addresses.

62. The apparatus according to claim 59, wherein the guard device is adapted to detect the pattern by detecting a large number of packets transmitted by the computer to a specified port.

63. Apparatus for processing communication traffic, comprising a guard device, which is adapted to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection,

to detect an increase in a rate of arrival of the packets that are indicative of the communication failure, and responsively to the increase, to filter the communication traffic so as to remove at least some of the communication traffic that is generated by the worm infection.

64. The apparatus according to claim 63, wherein the guard device is adapted to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure.

65. The apparatus according to claim 63, wherein the guard device is adapted to detect failures to establish a Transmission Control Protocol (TCP) connection.

66. Apparatus for processing communication traffic, comprising a guard device, which is adapted to monitor the communication traffic on a network so as to detect ill-formed packets, to make a determination, responsively to the ill-formed packets, that at least some of the communication traffic has been generated by a worm infection, and responsively to the determination, to filter the communication traffic so as to remove the at least some of the communication traffic that is generated by the worm infection.

67. The apparatus according to claim 66, wherein the packets comprise a header specifying a communication protocol, and wherein the guard device is adapted to detect that the packets contain data that are incompatible with the specified communication protocol.

68. The apparatus according to claim 66, wherein the packets comprise a header specifying a packet length, and

wherein the guard device is adapted to detect that the packets contain an amount of data that is incompatible with the specified packet length.

69. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor communication traffic that is directed to a group of addresses on a network, to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group, to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, such that the deviation is indicative that at least some of the communication traffic may be of malicious origin, and responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin.

70. The product according to claim 69, wherein the instructions cause the computer to select a subset of the group of the addresses to monitor responsively to the baseline characteristics.

71. The product according to claim 70, wherein the respective baseline characteristics are indicative of respective amounts of the communication traffic that are directed to the addresses in the group, and wherein the instructions cause the computer to select the addresses in the subset such that the addresses in the subset

receive relatively small amounts of the communication traffic by comparison with other addresses in the group.

72. The product according to claim 69, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic.

73. The product according to claim 69, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed.

74. The product according to claim 69, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic.

75. The product according to claim 69, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group.

76. The product according to claim 69, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic.

77. The product according to claim 76, wherein instructions cause the computer to read a Time-To-Live (TTL) field in headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems.

78. The product according to claim 69, wherein the instructions cause the computer to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network.

79. The product according to claim 78, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection.

80. The product according to claim 69, wherein the instructions cause the computer to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets.

81. The product according to claim 80, wherein the packets comprises Internet Control Message Protocol (ICMP) unreachable packets.

82. The product according to claim 69, wherein the instructions cause the computer to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets.

83. The product according to claim 69, wherein the instructions cause the computer to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count.

84. The product according to claim 83, wherein when the computer is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, the instructions cause the computer to determine an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the

count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address.

85. The product according to claim 84, wherein the instructions cause the computer to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address.

86. The product according to claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type.

87. The product according to claim 86, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port.

88. The product according to claim 86, wherein the instructions cause the computer to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses.

89. The product according to claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to

collect specific information relating to the traffic of the detected type.

90. The product according to claim 89, wherein the specific information comprises one or more source addresses of the traffic of the detected type.

91. The product according to claim 69, wherein the instructions cause the computer to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

92. The product according to claim 91, wherein the instructions cause the computer to monitor the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program.

93. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic originating from a group of addresses and passing through a selected node on a network, to detect a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses, and to trace a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running.

94. The product according to claim 93, wherein the instructions cause the computer to identify a port of a switch on the network to which the computer is connected, and to instruct the switch to disable the identified port.

95. The product according to claim 93, wherein the instructions cause the computer to detect the pattern by determining that the computer has transmitted packets to a large number of different destination addresses.

96. The product according to claim 93, wherein the instructions cause the computer to detect the pattern by detecting a large number of packets transmitted by the computer to a specified port.

97. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection, to detect an increase in a rate of arrival of the packets that are indicative of the communication failure, and responsively to the increase, to filter the communication traffic so as to remove at least some of the communication traffic that is generated by the worm infection.

98. The product according to claim 97, wherein the instructions cause the computer to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure.

99. The product according to claim 97, wherein the instructions cause the computer to detect failures to establish a Transmission Control Protocol (TCP) connection.

100. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect ill-formed packets, to make a determination, responsively to the ill-formed packets, that at least some of the communication traffic has been generated by a worm infection, and responsively to the determination, to filter the communication traffic so as to remove the at least some of the communication traffic that is generated by the worm infection.

101. The product according to claim 100, wherein the packets comprise a header specifying a communication protocol, and wherein the instructions cause the computer to detect that the packets contain data that are incompatible with the specified communication protocol.

102. The product according to claim 100, wherein the packets comprise a header specifying a packet length, and wherein the instructions cause the computer to detect that the packets contain an amount of data that is incompatible with the specified packet length.